DEPARTMENT OF FINANCE

ARNOLD SCHWARZENEGGER, GOVERNOR

915 L STREET ■ SACRAMENTO CA ■ 95814-3706 ■ WWW.DOF.CA.GOV

October 6, 2006

Mr. Kenneth J. O'Brien, Executive Director
Commission on Peace Officer Standards and Training
1601 Alhambra Boulevard
Sacramento, CA 95816-7083

Dear Mr. O'Brien:

Final Report—Internal Control Risk Assessment

Enclosed is the final report on our internal control risk assessment of the Commission on Peace Officer Standards and Training (Commission). This assessment was performed under an interagency agreement between the Commission and the Department of Finance to facilitate compliance with the Financial Integrity and State Manager's Accountability Act of 1983. The report identifies strengths and risks in the Commission's accounting and administrative controls, and recommends actions to reduce these risks.

The Commission's response is included in the enclosed report. Implementation of the proposed corrective actions will help strengthen the Commission's internal control and improve fiscal operations.

We appreciate the Commission's assistance with our assessment. If you have any questions regarding this report, please contact Richard R. Sierra, Manager, at (916) 322-2985.

Sincerely,

Original signed by:

Diana L. Ducay, Chief
Office of State Audits and Evaluations

Enclosure

cc: Mr. Dick Reed, Assistant Executive Director, Administrative Services Division, Commission on Peace Officer Standards and Training
Mr. Thomas Liddicoat, Chief, Administrative Services Bureau, Commission on Peace Officer Standards and Training
Ms. Karen Cramer, Budget Officer, Administrative Services Bureau, Commission on Peace Officer Standards and Training

A Risk Assessment

Commission on Peace Officer Standards and Training

Accounting and Administrative Controls

Prepared By:
Office of State Audits and Evaluations
Department of Finance

068120072DCR

April 2006

Table of Contents

PREFACE

The Department of Finance, Office of State Audits and Evaluations, conducted this risk assessment at the request of the Commission on Peace Officer Standards and Training (Commission). The objective was to assess the Commission's control of fiscal activities.

The Commission, established by the Legislature in 1959, sets minimum selection and training standards for California law enforcement, and functions under the direction of an appointed Executive Director. The Commission provides services and benefits to more than 600 participating agencies, including job related assessment tools, research on improved officer selection standards, management counseling services, development of new training courses, leadership training programs, and training reimbursement.

This report is intended solely for the information and use of the Commission. However, this report is a matter of public record and its distribution is not limited.

STAFF:

Richard R. Sierra, CPA
Manager

Doris M. Walsh
Supervisor

Ifeanyi Maduchukwu, CPA
Robert Castillo

As of April 13, 2006, strengths were noted in the Commission's income/expenditure, fixed assets, and information security functions. The Commission has well-documented policies and procedures that play an important part in risk management. There were also a few areas of elevated risk where corrective action is needed to minimize the potential for material errors, irregularities, and loss of assets, as noted below.

Cash Receipts and Disbursements: Endorsement safeguards and separation of duties could be strengthened to protect collections and disbursements from loss, theft, or misappropriation.

Accounts Receivable: Audit assessments are not recorded in the Commission's accounting system, and are collected from local agencies through an informal offset process. As a result, there is reduced assurance that all amounts due are recorded and collected, and that year-end financial statements accurately report the receivables balance.

Fixed Assets: The Commission has not completed a physical property inventory and reconciliation within the last three years, and may be unable to support the recorded asset balances.

Information Technology: The Commission has not completed a risk assessment of its information systems and does not require passwords to access the reimbursement application. As a result, information assets may be susceptible to theft, loss, or misuse.

DEPARTMENT OF FINANCE

ARNOLD SCHWARZENEGGER, GOVERNOR

915 L STREET ■ SACRAMENTO CA ■ 95814-3706 ■ WWW.DOF.CA.GOV

MANAGEMENT LETTER

Mr. Kenneth J. O'Brien, Executive Director
Commission on Peace Officer Standards and Training
1601 Alhambra Boulevard
Sacramento, CA 95816-7083

We have completed a risk assessment/limited review of the Commission on Peace Officer Standards and Training's accounting, administrative, and fiscal information security controls in effect as of April 13, 2006. Our scope was to assess relative risks in the above-mentioned controls and did not constitute a comprehensive study and evaluation of the internal controls. We applied procedures to the extent we considered necessary; this included observations, analyses, interviews, and limited transaction tests. We did not assess programmatic controls over the operation and performance of the Commission's mandated activities.

As summarized in the *Risks and Recommendations* section of this report, our assessment identified a number of internal control strengths and potential risks in the Commission's fiscal activities.

Commission management is responsible for establishing and maintaining adequate internal controls. The objective of internal controls is to provide reasonable, but not absolute, assurance that assets are safeguarded against loss from unauthorized use or disposition, and that transactions are executed in accordance with state control procedures, and recorded properly.

This report is intended solely for the information and use of Commission management. However, this report is a matter of public record and its distribution is not limited.

Original signed by:

Diana L. Ducay, Chief
Office of State Audits and Evaluations

April 13, 2006

Scope and Methodology

The Department of Finance, Office of State Audits and Evaluations, conducted this risk assessment/limited internal control review at the Commission's request. The assessment's purpose was to identify strengths and risks in the Commission's accounting, administrative, and fiscal information security controls. Accounting and administrative controls comprise management's plan to ensure the safeguarding of state assets through adequate segregation of duties, restricted access, authorization, record keeping, polices and procedures, employment of qualified personnel, and internal review. Fiscal information security controls are designed to protect information assets, and include electronic data processing security, data integrity, risk management, and disaster recovery planning. We performed the following procedures:

- Verified operable internal controls, including but not limited to, processes and procedures for staff use, methods of assigning authority and responsibility, segregation of duties, and personnel policies and practices.
- Identified the risks of material misstatement in the accounting records due to error or fraud, and identified and evaluated internal controls by transaction cycle.
- Determined compliance with state information security and risk management policies applicable to fiscal transaction processing, including the appointment of an information security officer and effective disaster recovery planning.
- Identified areas of operations that are subject to risk from inadequate controls or non-compliance with established controls, and recommended corrective action to minimize these risks.
- Followed-up on findings identified in our 2001 assessment report, determined whether those findings had been corrected, and evaluated the effectiveness of corrective actions.

We did not review programmatic controls over the operation and performance of the Commission's activities. Program controls include management's plan to ensure the efficient and effective operation of the Commission's activities and programs, the achievement of desired results or benefits, and compliance with applicable laws and regulations.

To complete the above procedures, we: (1) interviewed Commission staff and management; (2) reviewed accounting processes, administrative policies and procedures, information technology disaster recovery plans, and organization charts; (3) observed the safeguarding of cash receipts and blank check stock; (4) performed limited testing of bank reconciliations, timely and accurate recording of cash receipts, cash deposits, and remittances to the State Treasurer; and (5) reviewed and tested, on a limited basis, processes over purchasing, cash disbursements, equipment inventory, and claim schedules.

The following section includes our conclusions on control strengths and risks. The noted risks highlight areas warranting management attention.

Income and Expenditure Cycles

Effective receipt controls ensure that collections are adequately safeguarded and promptly recorded, subsidiary records are reconciled with control accounts and bank statements, and full cost recovery policies are followed. Effective disbursement controls ensure that all disbursements are properly approved and accurately recorded, checks and other negotiable instruments are safeguarded, check signing equipment is adequately controlled, disbursements are made only for allowable purposes, and bank accounts are timely reconciled.

Strengths

- Cash receipts are deposited timely and recorded accurately.
- Remittances to the State Treasurer are timely and accurate.
- Incoming collections are pre-listed.
- The collection process is centralized in the mail room.
- Cash disbursement policies and procedures are adequately documented.
- Cal-card use is appropriately restricted.
- Signature authorities are at appropriate levels and consistently applied.

Risk Area 1—Cash Receipt and Disbursement Duties Should Be Better Segregated

The following conflicting duties may create opportunities for undetected loss, theft, or misappropriation.

One accounting office employee receives collections and prepares deposits, inputs receipts and disbursements into the accounting system, reconciles bank accounts, and has access to blank checks. Conflicts arise when the same person that physically handles receipts also has control over major portions of the accounting process (e.g. posting cash transactions and reconciling accounts), while also having access to blank checks.

State Administrative Manual (SAM) Section 8080.1 states that no one person will perform more than one of the following duties:

1. Receiving and depositing remittances.
2. Inputting disbursement information.
3. Inputting receipts information.
4. Controlling (or having access to) blank check stock.
5. Reconciling accounts.

Calstars Procedures Manual, Volume 1, Chapter 19, Exhibits XIX-1 and XIX-2 contain useful matrices for separating duties in small organizations. These separations will help minimize risk and increase the likelihood that errors or irregularities will be discovered through reconciliations and normal operations.

Recommendation 1

Reassign duties so that the person receiving collections and preparing deposits does not reconcile bank accounts, input transactions, or have access to blank checks. Non-accounting employees may be used, when necessary and appropriate, to minimize incompatible duties.

Risk Area 2—Collections are Not Adequately Protected From Theft or Loss

Checks are not immediately endorsed upon receipt, and sometimes remain unendorsed in the mail room overnight before transfer to the accounting office. Unendorsed checks may create opportunities for theft or misappropriation, and timely endorsements serve to discourage the use of lost or stolen negotiable instruments.

SAM Section 8034.1 requires agencies to endorse checks, warrants, money orders, and other negotiable instruments on the day they are received.

Recommendation 2

Require all negotiable instruments to be immediately transferred to the accounting office for prompt endorsement on the day received. If unable to ensure timely transfer, then require the person who opens the mail to promptly endorse checks upon receipt.

Risk Area 3—Amounts Due From Local Agencies are Not Recorded As Receivables in the Accounting System

Audit assessments totaling $62,468 were not recorded as accounts receivable in the Commission's accounting system. As a result, there is no assurance that all amounts due are recorded and collected, and that year-end financial statements accurately report the receivables balance. Some balances remained uncollected for more than six months.

The Commission collects these assessments from local agencies through an informal offset process; however, this process is manual, not fully documented, and exclusively controlled by one employee. There is no written policy regarding local agencies' obligation to clear overpayments timely and completely, and agencies are not required to send checks to the Commission. Instead, the Commission deducts amounts due from a future reimbursement claim, which may be several months later.

This risk was also noted in our 2001 review.

SAM Section 8286 requires audit assessments to be established in the accounting records as a contingent receivable upon initial assessment, and that such receivables be fully deferred. Upon being made final, audit assessments will be recognized as valid receivables.

Recommendation 3

Record audit assessments as accounts receivables in the official accounting records. Establish and communicate to local agencies the procedures for collecting assessments, and require timely collection. If the Commission determines that the current manual tracking process is sufficient for the volume and frequency of assessments, then it should transfer the manual spreadsheet balance to the general ledger receivables account monthly or quarterly.

Fixed Assets Cycle

Effective fixed asset controls ensure that acquisitions and dispositions are properly authorized and timely recorded, accurate asset accountability is maintained, physical inventories are periodically conducted, and subsidiary records are reconciled with control accounts.

Strengths

- Equipment acquisitions are properly authorized.
- Equipment is capitalized according to SAM criteria, and is tracked in a database.

Risk Area 4—A Physical Inventory Has Not Been Completed

The Commission has not completed a physical inventory of its property and reconciled the inventory count to the accounting records. As a result, it may be unable to maintain adequate control and accountability over fixed assets, or prevent undetected theft of property.

SAM Section 8652 requires departments to make a physical count of all property and reconcile the count with the accounting records at least once every three years, and to maintain evidence of the physical inventory.

Recommendation 4

Conduct a physical inventory of all Commission property and reconcile the account with the accounting records. Ensure that the inventory process is repeated at least once every three years.

Information Security

Effective information technology controls ensure that access to accounting system hardware and software is adequately controlled, data integrity is maintained, operational continuity plans exist, and key person dependency is avoided.

Strengths

- Hardware, software, and computer use polices are properly documented.
- A current Operation Recovery Plan is on file with the Department of Finance.

Risk Area 5—Information System Access and Risk Assessment Procedures Could Be Improved

The POST Information System does not require password and user identification to access the reimbursement application. Also, the system does not automatically log-off when not in use. Because the reimbursement application contains confidential peace officer information and financial data, it should be adequately protected from unauthorized use, modification, access, or disclosure.

Although the Commission completed an Operational Recovery Plan to deal with potential disasters, it has not conducted a system-wide risk assessment of vulnerabilities and consequences associated with daily operations, such as physical security and access,

programming, systems documentation, protection of confidential information, separation of duties, and system reliability.

SAM Section 4840 requires agencies to ensure the integrity of computerized information resources by protecting them from unauthorized access, modification, destruction, or disclosure, and to ensure the physical security of these resources.

SAM Section 4842.1 requires all agencies to establish a risk analysis process to identify and assess risks associated with its information assets and develop a cost-effective approach to managing those risks.

Recommendation 5

Require user identifications and passwords to access the reimbursement application. Conduct a system-wide risk analysis to identify, assess, and manage risks associated with the Commission's information assets.

Conclusion

Strengths were apparent in a number of areas, indicating that the Commission has taken appropriate steps to manage its accounting, administrative, and fiscal information systems and controls. The Commission recognizes and communicates to its employees the importance of maintaining effective internal controls. To assist the Commission with its ongoing risk management program, we identified areas of potential risk and recommended corrective actions to reduce these risks.

Our work was limited to those areas specified in the *Scope and Methodology* section of this report, based on fieldwork performed between March 9, 2006 and April 13, 2006.

State of California Department of Justice

M e m o r a n d u m September 13, 2006

To: Doris M. Walsh, Supervisor
Office of State Audits and Evaluations
Department of Finance
915 L Street
Sacramento, CA 95814-3706

From: Thomas S. Liddicoat, Chief
Administrative Services Bureau
Commission on Peace Officer Standards and Training

Subject: Responses to Draft Report – Internal Control Risk Assessment

The Commission on Peace Officer Standards and Training (POST) does herewith submit the following as its responses to the draft report on the internal control risk assessment (copy attached) performed by your department.

Risk Area 1 – Cash Receipt and Disbursement Duties.

POST agrees with the recommendation to reassign duties, even though it will be to non-accounting employees, in order to be able to satisfy SAM requirements and reduce possible risks. Training will be needed for the new duties.

Each of the following duties will be reassigned to a different staff person:

Controlling blank check stock
Endorsing checks
Write receipts/Prepare deposit
Inputting disbursements information
Inputting receipts information
Input cash remittance information (SCO journal entry)
Reconciling accounts (Gen. Fund & Rev. Fund)

Risk Area 2 - Collections are Not Adequately Protected From Theft or Loss

POST's mail clerk now promptly endorse checks upon receipt.

Risk Area 3 – Amounts Due From Local Agencies are Not Recorded as Receivables

POST will accrue amounts due from local agencies at year-end, the amount to be provided by staff in the Reimbursement Unit. This was an agreed upon solution at the exit conference with the Finance auditors.

Risk Area 4 – A Physical Inventory Has Not Been Completed

POST is a small agency with approximately 121 staff members. Over 3 years ago the Contract Officer was called to military service, and her position at POST remained vacant until March 2006. A complete physical inventory has not been conducted due to staffing shortages.

POST reconciles its property inventory with the Accounting Unit on a monthly basis. POST maintains a data system (Equipo) to record all property tag numbers and the location of all items. A report is prepared monthly and reviewed by the Accounting Unit.

POST will establish a new procedure to conduct a complete property inventory to comply with SAM section 8652.

1. Staff will establish an "equipment list" to determine which items require a property tag.
2. Staff will establish a count method procedure.
3. Staff will establish a schedule for quarterly inventory by Bureau.
4. Staff will reconcile the property inventory list with Accounting on a quarterly basis (Bureau property list) and a complete list (from all Bureau lists) every three years.

When items are broken or obsolete, POST processes a STD 152 form (Property Survey Report) and transfers the items to the Department of General Services, Property Reutilization. Upon acceptance and approval of the STD 152 form, the item is deleted from the POST Equipment Inventory. This process occurs on an "as needed" basis.

POST will establish the property inventory procedure and conduct a physical inventory during the 06/07 fiscal year.

Risk Area 5 – Information System Access and Risk Assessment Procedures

***DOF**: The POST Information System does not require password and user identification to access the reimbursement application.*

POST requires a user ID and password to connect any PC (inside POST) to the POST Network. The user ID then determines which applications the user is provided. Therefore, POST does require a password and user identification to access the reimbursement application.

***DOF**: Also, the system does not automatically log-off when not in use.*

The POST Internal Manual (PIM) addresses this issue and at one time we required automatic log-offs or screen savers with passwords. Over the past few years, POST staff have not kept their screen saver passwords enabled. POST PIM A-30 states "Employees with access to the POST Peace Officer Database are required to use a password protected screen saver with a 10 or less minute wait setting."

POST has now taken steps to address the observation by DOF and now requires users to have a screen saver with a password set to 10 minutes. This has been implemented.

***DOF**: Although the Commission completed an Operational Recovery Plan to deal with potential disasters, it has not conducted a system-wide risk assessment of vulnerabilities and consequences associated with daily operations, such as physical security and access, programming, systems documentation, protection of confidential information, separation of duties, and system reliability.*

POST has entered into a contract with Hubbard Systems to perform a thorough IT Risk Assessment. Hubbard systems delivered their first draft of the IT Risk Assessment report on August 28, 2006 for review. The final report will be completed by October 31, 2006. Upon receiving the final report, POST staff will make recommendations to address all potential risks reported in the IT Risk Assessment report.

Please feel free to call me at (916) 227-3928 should you have any questions.

Attachment